JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11)Publication number: 10039753
(43)Date of publication of application: 13.02.1998

(51)Int.Cl.
G09C 1/00
H04L 9/32

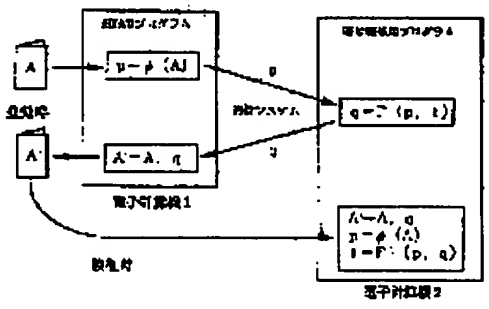
(21)Application number: 08222994
(22)Date of filing: 23.07.1996

(71)Applicant: OOTA TERUHITO
(72)Inventor: OOTA TERUHITO

(54) METHOD FOR IMPARTING DETERMINISTIC DATE TO ELECTRONIC INFORMATION

(57)Abstract:

PROBLEM TO BE SOLVED: To make it possible to impart deterministic date to an electronic file by sending the enciphered date back to an electronic computer and previously linking the electronic file and the date on a recording medium.
SOLUTION: A user calculates an identification value p from the electronic file A for imparting the date by using the function ψ supplied from an entrepreneur by using the electronic computer 1 having a sufficient calculation capability and sends the value to the entrepreneur by a communication system. The entrepreneur encrypts the value (t) indicating the date of the point of the time with (p) as a key by using the electronic computer 2 having the sufficient calculation capability and sends the encrypted date (q) again back to the user by using the communication system. The user keeps the date (q) in linkage to the original electronic file A. When a need arises, the user carries the electronic file A' imparted with the date to the place of the entrepreneur. The entrepreneur calculates the identification value (p) again from A' by using the function ψ and obtains the date (t) by decrypting (q) with the resulted (p) as the key.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁(JP)　(12)公開特許公報（A）　(11)特許出願公開番号

特開平１０－３９７５３

(43)公開日　平成10年(1998)2月13日

(51)Int.Cl.[6]		識別記号	庁内整理番号	FI			技術表示箇所
Ｇ０９Ｃ	1/00	６４０	7259－５Ｊ	Ｇ０９Ｃ	1/00	６４０　Ｚ	
Ｈ０４Ｌ	9/32			Ｈ０４Ｌ	9/00	６７５　Ｚ	

審査請求　未請求　請求項の数１　書面　（全３頁）

(21)出願番号　特願平８－２２２９９４

(22)出願日　平成8年(1996)7月23日

(71)出願人　596111221
太田　暉人
千葉県千葉市中央区葛城一丁目9番11号

(72)発明者　太田　暉人
千葉県千葉市中央区葛城一丁目9番11号

(54)【発明の名称】電子情報への確定日付付与法

(57)【要約】
【目的】電子ファイルに確定日付を付与すること。
【方法】２機の電子計算機を通信回線を通じてつなぎ、利用者の電子ファイルから計算される同定値を事業者に送り、事業者はこれを鍵として日付を暗号化し、結果を利用者にもどしてもとの電子ファイルにリンクさせておく。

1

【特許請求の範囲】

電子計算機１を用いて、対象物である電子ファイルＡから所定の方法で同定値ｐを算出して、その値を通信システムを介してもうひとつ別の電子計算機２に送り、当該計算機を用いてｐを鍵にして日付を表す値ｔを暗号化し、暗号化された日付ｑを再び電子計算機１に送り返し、記録媒体上でＡとｑとをリンクさせておくことによって、Ａに確定日付を付与する方法。

【発明の詳細な説明】

本発明は、記録媒体上の情報がある時点で既に存在していたことを証明するための確定日付を付与する方法を提供するものである。知的所有権の保護の拡大により、ある知見やアイディアが、ある時点で既に存在したことを証明する必要が非常に大きくなっている。たとえば平成８年１月１日付けの米国特許法の改正により米国外でなされた発明に対しても先発明主義が適用されることになり、米国での特許係争を想定する場合は、研究の場でその発明がいつなされたか文書上の証拠として残す必要が生じてきている。これまで、日本の国内で一般に認められた情報の存在証明法は、その情報を記載した書類を公正証書役場において、確定日付の押捺を受けることである。一方、電子計算機の普及により、非常に多くの情報が、記録媒体のデイジタルな符号として存在することが非常に多くなっている。しかしながら、記録媒体にデイジタルな符号として記録された情報（以下、電子ファイルという。）は、書換が容易であるため、証拠能力のある形で日付を付与することは困難であった。電子ファイルの内容をそっくり、第三者に預託しておく方法も考えられるが、日付を確定する必要のあるものは、往々にして機密性の高いものが多く、第三者を通して洩れる心配を考えると利用者にとって利用しにくいし、預託される側も膨大な量の情報を保管管理することになり現実的とは言えない。本発明は、電子計算機の高い計算能力と通信システムを利用して、一種の暗号方式を用いて、情報本体をを外部に出すことなく、記録媒体中の情報に確定日付を付与するものである。日付の付与は、サーヴィスの提供者（以下、事業者という。）と利用者とに分かれて以下の手順で行う。

１）利用者は、十分な計算能力を有する電子計算機１を使い、事業者から供給された関数ϕを用いて日付を付与しようとする情電子ファイルＡから、同定値ｐを算出し、この値を通信システムを用いて事業者に送る。

$p=\phi(A)$

２）事業者は、ｐの値を受け取り、十分な計算能力を有する電子計算機２を用いて、ｐを鍵としてその時点の日付を表す値ｔを暗号化して、暗号化された日付ｑを再び通信システムを用いて利用者に送り返す。

$q=F(p, t)$

暗号化する関数Ｆは利用者が知ることができない状態におかれる。

2

３）暗号化された日付ｑを受け取った利用者は、これをもとの電子ファイルＡとリンクして記録しておく。

$A'=A, q$

必要が生じたら利用者は、日付を付与された電子ファイルＡ’を事業者のところに持ち込み、事業者は以下の手順で確定日付を確認する。すなわち、Ａ’からＡとｑとを分離し、Ａから再び関数ϕを用いて同定値ｐを計算し、得られたｐを鍵としてｑを復号して日付ｔを得る。

$t=F^{1}(p, q)$

もし、この時点までにＡ’の中身が改竄されていれば、同定値ｐの値も変わるので、もとのｔの値を再現することはできない。このようにして利用者は、電子ファイルＡが過去の特定の日付に既に存在しており、しかもその後中身が変更されていないことを、第三者に合理的に証明してもらうことができる。電子ファイルの内容は、文書でも、図形でも、計算プログラムでも、ゲームソフトでもなんでも良い。関数ϕは、ファイルＡから、一定の演算を経て同定値ｑを導くもので、ｑの値を変えずにＡの中身を変更する手段が容易に得られるようなものであってはならない。一般にハッシュ関数と呼ばれるものがϕとして利用可能である。ハッシュ関数は、一般に通信時に電文が改竄されていないことを確認するために用いるもので、任意のサイズのテキストから、繰り返し演算によって所定のビット数の値を得るもので、ビット数が大きくなると、同じ値を持つ異なるテキストを求めるのが極端に困難になることが知られている。関数Ｆは、同定値ｐを用いて時刻を表す値ｔを暗号化するもので、一般に用いられる暗号用の関数であればよい。また、日付を表す値ｔは、その時点での日付や時間に対応していればよく、過去のある時点を起点にして秒単位で数えるシリアル数を用いることができる。この計算に用いる電子計算機１、２は、それぞれ限られた時間内に関数ϕ、関数Ｆを計算するのに十分な計算能力を有していなくてならない。通常のサーヴィスを考えると、１件の登録にかけられる時間は、登録するファイルが極端に大きくない限り、せいぜい１時間、好ましくは１０分以内であるので、電子計算機１、２ともに１ＭＩＰＳ（１秒間に１００万命令を実行する能力）以上、好ましくは１０ＭＩＰＳ以上は必要である。通信システムとは、電線、光ファイバー、空間もしくは、それらの組み合わせにより信号を空間的に離れた場所に送るためのシステムのことで、特にここではインターネットなど、広域にわたり多数の利用者が利用できるシステムを意味している。記録媒体上でＡとｐをリンクするとは、記録媒体上のＡの所在を知ればｑの所在が分かるか、あるいは、ｑの所在を知ればＡの所在を分かるように配置しておくか、あるいはまた、あるデータをみるとＡとｑの所在が同時に分かる様にしてあることをいう。Ａとｑとは必ずしも同一媒体上にある必要はないが、管理上はｑをＡの機能を妨げない形式でＡと記録媒体上同一の位置に配置

して、単一ファイルとして扱うことが好ましい。この方法の特長は以下の通りである。

１）日付を確定する必要がある資料は、往々にして機密性のものが多いと思われるが、利用者は、登録するファイルの中身を事業者に知らせる必要もなければ、通信回線を介して送信する必要もない。

２）事業者は、登録に関する一切の情報を自ら保管する必要がない。

３）ファイルＡ'はファイルＡと同様に機能するので、利用者は登録後、Ａ'をＡに代えてそのまま利用できる。即ち、これは電子ファイルＡ上にｐという日付印を

押したことに実質的に同じである。

【図面の簡単な説明】

【図１】は、本発明に従って、電子ファイルに日付を付与する時と、それを検証する時の計算の流れを表す。図中、Ａ及びＡ'は、元の電子ファイル及び日付を付与された電子ファイルを表し、ｐ、ｔ、ｑはそれぞれファイルＡの同定値、日付、暗号化された日付を表す。また、関数ϕ、関数Ｆ、関数F^{-1}は、それぞれ、元のファイルから、そのファイルの同定値を求めるための関数、日付を同定値で暗号化する関数、及び復号する関数を表す。

【図１】